CLAIMS

1. A network system for determining trivial keyboard sequences of a proposed password, comprising:

a user system;

a computer keyboard input device associated with said user system;

a server in communication with said user systems via a communications link;

a data storage device coupled to said server, said data storage device housing:

a database including a keyboard profile wherein said keyboard profile specifies a physical layout of character and function keys on said computer keyboard input device;

a master password database including a user account associated with said user system; and

a password verification mechanism executable by said server;

wherein, upon execution, said password verification mechanism performs an algorithm on said proposed password and determines triviality of said proposed password according to criteria specified in said algorithm.

2. The network system of claim 1, wherein said physical layout of character and function keys is specified by:

a graphical representation of said computer keyboard input device;

an X axis horizontally spanning said graphical representation;

a Y axis vertically spanning said graphical representation;

wherein each of said character and function keys is assigned a unique data coordinate set identifying positional placement values.

3. The network system of claim 1, further comprising an identifier assigned to said keyboard profile, said identifier indicating manufacturer and model data.

4. The network system of claim 3, wherein said identifier is associated with corresponding user accounts via said master password database.

5. The network system of claim 4 wherein, upon initiating a proposed password request by a user system, said password verification mechanism automatically retrieves a keyboard profile associated with said user system via said identifier.

6. The network system of claim 1, wherein said algorithm comprises three formulas wherein:

a first formula checks for vertical triviality of said proposed password;

a second formula checks for horizontal triviality of said proposed password; and

a third formula checks for diverse keystroke patterns of said proposed password;

wherein said second formula is executed upon successful validation of said first formula; and said third formula is executed upon successful validation of said second formula.

7. The network system of claim 6, wherein successful validations of any of said three formulas causes said password verification mechanism to:

transmit notification to at least one of:

a requesting user system; and

an administrator system; and

update said master password database.

8. The network system of claim 1, wherein said server and said data storage device comprise one unit.

9. A keyboard profile operable for facilitating triviality determination of proposed passwords, comprising:

a graphical representation of a computer keyboard, said representation including character and function keys;

an X axis horizontally spanning said graphical representation;

a Y axis vertically spanning said graphical representation;

wherein each of said character and function keys is assigned a unique data coordinate set identifying positional placement values; and

an identifier indicating manufacturer and model data of a computer keyboard associated with said profile;

wherein a password verification mechanism executes an algorithm on data coordinates assigned to a proposed password resulting in a determination of triviality.

10. The keyboard profile of claim 10 wherein said triviality is determinable by at least one of:

non-acceptable distances between said data coordinates; and

non-acceptable sequences of said data coordinates as positioned on said computer keyboard, and wherein further, standards for said non-acceptable distances and non-acceptable sequences are provided by said password verification mechanism.

11. A method for determining keyboard triviality of proposed passwords over a network system, comprising:

receiving a request for a proposed password from a user system;

retrieving user account data related to said user system;

checking said proposed password against existing password quality rules stored in a master password database, wherein a requester of said proposed password is redirected to select an alternative password if said checking results in an unacceptable password;

providing a keyboard profile associated with said user system, said keyboard profile including a unique identifier;

performing an algorithm on said proposed password, said algorithm including a first formula, comprising:

$(\triangle X1 + \triangle X2 + \ldots + \triangle Xn - 1)/(n - 1) > 0;$

wherein:

X represents an X axis;

Y represents an Y axis;

n represents a number of characters comprising said proposed password; and

$\triangle X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

and wherein further data coordinates are plugged into said first formula for determining vertical triviality.

12. The method of claim 11, wherein said algorithm includes a second formula executable upon successful completion of said first formula, comprising:

$(\triangle Y1 + \triangle Y2 + \ldots \triangle Yn - 1)/(n - 1) > 0;$

wherein:

X represents an X axis;

Y represents a Y axis;

n represents a number of characters comprising said proposed password; and

$\triangle Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis;

and wherein further data coordinates are plugged into said second formula for determining horizontal triviality.

13. The method of claim 11, wherein said algorithm includes a third formula, comprising:

$(\triangle X1 + \triangle Y1 + \triangle X2 + \triangle Y2 + \ldots + \triangle Xn - 1 + \triangle Yn - 1)/(2(n - 1)) >= S;$

wherein:

X represents an X axis;

Y represents a Y axis;

n represents a number of characters comprising said proposed password;

$\triangle X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

$\triangle Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis; and

S represents a variable parameter representing a mean distance between character keys of proposed passwords;

and wherein further data coordinates are plugged into said third formula for determining diverse keystroke patterns of said proposed password.

14. The method of claim 13, wherein successful completion of said algorithm causes a password verification mechanism to:

transmit acceptance of said proposed password to at least one of:

said user system;

an administrator system; and

update a password database to reflect said acceptance.

15. The method of claim 11, wherein said identifier is linked to said user account, and wherein further, said keyboard profile is automatically provided over said network system via said link.

16. The method of claim 11, wherein a list of available keyboard profiles are presented to said user selection, and wherein further, said user system selects an appropriate profile.

17. A storage medium encoded with machine-readable computer program code for determining keyboard triviality of proposed passwords over a network system, the storage medium including instructions for causing said computer network to implement a method comprising:

receiving a request for a proposed password from a user system;

retrieving user account data related to said user system;

checking said proposed password against existing password quality rules stored in a master password database, wherein a requester of said proposed password is redirected to select an alternative password if said checking results in an unacceptable password;

providing a keyboard profile associated with said user system, said keyboard profile including a unique identifier;

performing an algorithm on said proposed password, said algorithm including a first formula, comprising:

$(\triangle X1 + \triangle X2 + ... + \triangle Xn - 1)/(n - 1) > 0;$

wherein:

X represents an X axis;

Y represents a Y axis;

n represents a number of characters comprising said proposed password; and

$\triangle X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

and wherein further data coordinates are plugged into said first formula for determining vertical triviality.

18. The storage medium of claim 17, wherein said algorithm includes a second formula executable upon successful completion of said first formula, comprising:

$(\triangle Y1 + \triangle Y2 + \ldots \triangle Yn - 1)/(n - 1) > 0;$

wherein:

X represents said X axis;

Y represents said Y axis;

n represents a number of characters comprising said proposed password; and

$\triangle Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis;

and wherein further data coordinates are plugged into said second formula for determining horizontal triviality.

19. The storage medium of claim 17, wherein said algorithm includes a third formula, comprising:

$\triangle X1 + \triangle Y1 + \triangle X2 + \triangle Y2 + \ldots + \triangle Xn - 1 + \triangle Yn - 1)/(2(n - 1)) >= S;$

wherein:

X represents said x axis;

Y represents said y axis;

n represents a number of characters comprising said proposed password;

$\triangle X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

$\triangle Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis; and

S represents a variable parameter representing a mean distance between character keys of proposed passwords;

and wherein further data coordinates are plugged into said third formula for determining diverse keystroke patterns of said proposed password.

20. The storage medium of claim 19, wherein successful completion of said algorithm causes a password verification mechanism to:

transmit acceptance of said proposed password to at least one of:

said user system;

an administrator system; and

update a password database to reflect said acceptance.

21. The storage medium of claim 17, wherein said identifier is linked to said user account, and wherein further, said keyboard profile is automatically provided over said network system via said link.

22. The storage medium of claim 17, wherein a list of available keyboard profiles are presented to said user selection, and wherein further, said user system selects an appropriate profile.